Manual
W2022ac, W2022ac-ext

Legal Notice

Warranty

This publication is subject to change.

bintec elmeg GmbH offers no warranty whatsoever for information contained in this manual. bintec elmeg GmbH is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

Chapter 1 Installation

Note

Please read the safety notices carefully before installing and starting up your device. These are supplied with the device.

1.1 W2022ac and W2022ac-ext

1.1.1 Setting up and connecting

Note

All you need for this are the cables supplied with the equipment.

The device **W2022ac** uses integrated antennas. Their radiation is optimized for ceiling mounting.

The device **W2022ac-ext** uses external antennas.

When setting up and connecting, carry out the steps in the following sequence:

(1) Antennas

For **W2022ac-ext** screw the provided standard antennas on to the connectors provided for this purpose.

(2) LAN

For the standard configuration of your device via Ethernet connect port **LAN1** of your device to your PC.
The device automatically detects whether it is connected to a switch or directly to a PC.
Select here only one of the connections **LAN1** or **LAN2**, the second connection is used to cascade several devices.
If you use more than one Ethernet connections on the same switch, loops may be formed.
The standard patch cable (RJ45-RJ45) is symmetrical. It is therefore not possible to mix up the cable ends.

(3) Power connection

Note

The devices are supplied without a mains unit. The power adapter with EU plug (part number 5500002091) is available as an accessory.

Connect the device to a mains socket. Use the power cord and insert it in the appropriate socket on your device. Now plug the power cord into a power socket (100–240 V). The status LED signal that your device is correctly connected to the power supply. Optionally, power can be supplied through a standard PoE injector (part number 5530000338).

Installation

The access points are to be mounted either on the wall, on the ceiling or used as a table-top devices.

Use as a table-top device

The device have integrated rubber pads. Place your device on a solid, level base.

Wall / Ceiling mounting

The devices are to be mounted by tabs on the back of the housing to the wall. A ceiling mount is available as an accessory to mount the device on the ceiling (article number 5520000163). The ceiling mount allows mounting on suspended system ceilings without drilling and dowels.

Warning

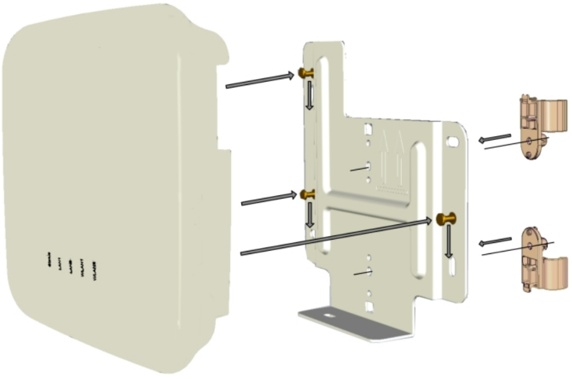
Before drilling, make sure that there are no building installations where you are drilling. If gas, electricity, water or waste water lines are damaged, you may endanger your life or damage property.

- Use the bracket as a template to mark out the drilling holes.
- Screw the bracket to the wall or ceiling with the provided dowels and screws.
- When mounting the unit to the struts of an intermediate ceiling, screw the supplied plastic clips to the back of the bracket.
- Connect all necessary cables (Ethernet, power supply) to the access point before inserting it into the bracket.

  Make sure that the cables are not a source of danger! Guide the cables through the cable guides!
- Fit the device onto the 3 metal pins and push it down until it clicks into place. When

mounting to an intermediate ceiling, push the plastic clips against the braces so that they click into place, too.

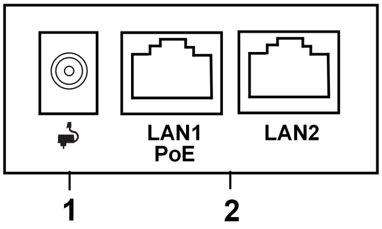
- If necessary, secure the device with a Kensington® lock against theft.



Ceilingmounting

1.1.2 Connectors

The connections are located on the underside of the device:



Underside

1	POWER	Socket for power supply
2	LAN1/PoE und LAN2	10/100/1000 Base-T Ethernet interfaces.

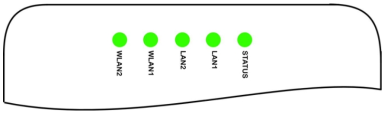
1.1.3 LEDs

The LEDs show radio status and radio activity of your device.

Note

Note that the number of active WLAN LEDs depends on the number of existing radio modules.

The LEDs are arranged as follows:



In operation mode, the LEDs display the following status information for your device:

LED status display

LED	Colour	Status	Information
Status		off	No power supply connected. Error if other LEDs are lit.
	green	on (flashing)	Normal operation
	red	on (static)	Failure
	red	on (flashing	Management communication error
LAN 1/2		off	No LAN
	yellow	on (static)	10 Mbit/s or 100 Mbit/s active
	yellow	on (flashing)	10 Mbit/s or 100 Mbit/s data traffic
	green	on (static)	1000 Mbit/s active
	green	on (flashing)	1000 Mbit/s data traffic
WLAN 1/2		off	Radio module and/or SSIDs inactive
	green	on (slowly blinking)	SSID active, no client is authenticated
	green	on (fast blinking)	SSID active, one or more clients authenticated
	green	on (flashing)	SSiD active, one or more clients authenticated and data traffic

You can choose from three different operation modes of the LEDs in the **System Management**->**Global Settings**->**System** menu.

Note

If you change the LED behavior through the **GUI**, this setting is preserved if you reset the device to the ex-works state.

Normal	All LEDs show their standard behavior.
Minimal	Only the status LED flashes once per second.

Off	All LEDs are deactivated.

1.1.4 Scope of supply

Your device comes with the following accessories:

	Cable sets/mains unit/other	Documentation
W2022ac	**W2022ac**	Installation poster Safety notices
W2022ac-ext	**W2022ac-ext** 4 external standard WLAN antennas	Installation poster Safety notices

1.1.5 General Product Features

The general product features cover performance features and the technical prerequisites for installation and operation of your device.

The features are summarised in the following table:

General Product Features

Property	Value
Dimensions and weights:	
Equipment dimensions without cable (W x D x H)	ca. 190 x 190 x 38 mm
Weight	approx. 505 g
LEDs	5 (1x Power, 2x WLAN, 2x Ethernet)
Power consumption of the device	max. 8.95 W
Voltage supply	12 V, 1.5 A (The power adapter with the part number 5500002091 is available as an accessory.) PoE an Ethernet 1 Class 0, according to 802.3af (max. 12.4 W). The Gigabit PoE Injector with part number 5530000082 is available as an accessory.
Environmental requirements:	
Storage temperature	-10 °C to +70 °C
Operating temperature	0 °C to +40 °C
Relative atmospheric humidity	10 % to 90 %
Available interfaces:	

Property	Value
WLAN	One radio module IEEE 802.11bgn MIMO 2x2 and a second radio module IEEE 802.11ac/an MU-MIMO 2x2 allow simultaneous operation at 2.4 and 5 GHz.
LAN/WAN	2 x 10/100/1000 mbps
PoE (Power-over-Ethernet)	Power-over-Ethernet according IEEE 802.3af, compatible with 802.3at PoE injectors
Available sockets:	
Ethernet interface	2 RJ45 sockets
Antennas:	
Antenna connection	**W2022ac**: Integrated single band MIMO antenna array with two antenna elements for each radio; 2 dBm gain @ 2,4 GHz; 3 dBm gain @ 5 GHz. **W2022ac-ext**: Two external antennas with omni characteristic for each radio module, RSMA socket, appr. 1,5 dBm
Transmit Power (WLAN)	max. 100 mW (20 dBm) EIRP
Standards & Guidelines	Directive 2014/53/EU, 2011/65/EU, 2009/125/EU, EN 60950-1; EN 62311; EN 301489-1; EN301489-17; EN 300 328; EN 301893; EN 50581; EN 60601-1-2 (Medical devices - part 1-2)
Buttons	Reset button for restart or reset

1.1.6 Reset

If the configuration is incorrect or if your device cannot be accessed, you can reset the device to the ex works standard settings using the reset button.

You can reset the access point to the ex works state in either of two ways:

(1) In the menu **Maintenance**->**Factory Reset**.

(2) Through the **reset button** on the side of the device.
Press the button until all LEDs are off, but the status LED that remains on.
As a protection against unauthorized use, the reset button may be covered by the mounting bracket. Remove the access point from the bracket in order to access the reset button.

Both methods delete all configurations and passwords.

You can now configure your device again as described from *Basic configuration* on page 9
.

Note

If you have changed the LED behavior to something other then the default value, this setting is preserved after resetting the device.

1.2 Cleaning

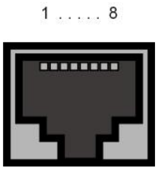
You can clean your device easily. Use a damp cloth or antistatic cloth. Do not use solvents. Never use a dry cloth; the electrostatic charge could cause electronic faults. Make sure that no moisture can enter the device and cause damage.

1.3 Pin Assignments

1.3.1 Ethernet interface

The devices **W2022ac** and **W2022ac-ext** have two 10/100/1000 Ethernet interfaces.

The connection is made via an RJ45 socket.



The pin assignment for the Ethernet 10/100/1000 Base-T interface (RJ45 socket) is as follows:

RJ45 socet for LAN connection

Pin	Function
1	Pair 0 +
2	Pair 0 -
3	Pair 1 +
4	Pair 2 +
5	Pair 2 -
6	Pair 1 -
7	Pair 3 +
8	Pair 3 -

1.4 Frequencies and channels

Different certification regulations apply around the world. ETSI standards generally apply (predominantly used in Europe). For operation in Europe, please read the notes in the RED Compliance Information.

1.5 Support information

If you have any questions about your new product, please contact a local, certified retailer for prompt technical support. Resellers have been trained by us and receive privileged support.

Further information on our support and service offers can be found on our web site.

Chapter 2 Basic configuration

You can use the **GUI** (other configuration steps) for the basic configuration of your device.

The basic configuration is explained below step-by-step. A detailed online help system gives you extra support.

This user's guide assumes you have the following basic knowledge:

- Basic knowledge of network structure
- Knowledge of basic network terminology, such as server, client and IP address
- Basic knowledge of using Microsoft Windows operating systems

You can find other useful applications at our web site.

2.1 Presettings

2.1.1 Preconfigured data

You have three ways of accessing your device in your network to perform configuration tasks:

(a) Dynamic IP address

In ex works state, your device is set to DHCP client mode, which means that when it is connected to the network, it is automatically assigned an IP address if a DHCP server is run. You can then access your device for configuration purposes using the IP address assigned by the DHCP server. For information on determining the dynamically assigned IP address, please see your DHCP server documentation.

(b) Fallback IP address

If you do not run a DHCP server, you can connect your device directly to your configuration PC and then reach it using the following, predefined fallback IP configuration:

- **IP Address**: *192.168.0.252*
- **Netmask**: *255.255.255.0*

Make sure that the PC from which the configuration is performed has a suitable IP configuration (see *Configuring a PC* on page 12).

(c) Assigning a fixed IP address

Use the following access data to configure your device in an ex works state:

- **User Name**: *admin*
- **Password**: *admin*

Note

All bintec elmeg devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. Make sure you change the passwords to prevent unauthorised access to your device!

How to change the passwords is described in *Modify system password* on page 14.

2.1.2 Software update

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You can easily perform an update with the **GUI** using the **Maintenance**->**Software &Configuration** menu.

For a description of the update procedure, see *Software Update* on page 15.

2.2 System requirements

For configuration, your PC must meet the following system requirements:

- Suitable operating system (Windows, Linux, MAC OS)
- A web browser (Internet Explorer, Firefox, Chrome) in the current version
- Installed network card (Ethernet)
- High colour display to show the graphics correctly
- TCP/IP protocol installed (see *Configuring a PC* on page 12)

2.3 Preparation

To prepare for configuration, you need to...

- Obtain the data required for the basic configuration.
- Check whether the PC from which you want to perform the configuration meets the necessary requirements.

2.3.1 Gathering data

The main data for the basic configuration can be gathered quickly, as no information is required that needs in-depth network knowledge. If applicable, you can use the example values.

Before you start the configuration, you should gather the data for the following purposes:

- IP configuration (obligatory if your device is in the ex works state)
- Configuration of a wireless network connection in Access Point mode

The following table shows examples of possible values for the necessary data. You can enter your personal data in the "Your values" column, so that you can refer to these values later when needed.

If you configure a new network, you can use the given example values for IP addresses and netmasks. In cases of doubt, ask your system administrator.

Basic configuration

For a basic configuration of your gateway, you need information that relates to your network environment:

IP configuration of the access point

Access data	Example value	Your values
IP address of your access point	*192.168.0.252*	
Netmask of your access point	*255.255.255.0*	

Access Point mode

If you run your device in Access Point mode, you can set up the required wireless networks. To do this, you need the following data:

Configuration of a wireless network

Access data	Example value	Your values
Network Name (SSID)	*default*	
Security mode	*WPA-PSK*	
Preshared key	*supersecret*	

2.3.2 Configuring a PC

In order to reach your device via the network and to be able to carry out configuration, the PC used for the configuration has to satisfy some prerequisites.

- Make sure that the TCP/IP protocol is installed on the PC.
- Select the suitable IP configuration for your configuration PC.

  The PC via which you want to configure the IP address for your device must be in the same network as your device.

Checking the Windows TCP/IP protocol

Proceed as follows to check whether you have installed the protocol:

(1) Click the Windows Start button and then **Settings** -> **Control Panel** -> **Network Connections** (Windows XP) or **Control Panel** -> **Network and Sharing Center**-> **Change Adapter Settings** (from Windows 7 on).

(2) Click on **LAN Connection**.

(3) Click on **Properties** in the status window.

(4) Look for the **Internet Protocol (TCP/IP)** entry in the list of network components.

Installing the Windows TCP/IP protocol

If you cannot find the **Internet Protocol (TCP/IP)** entry, install the TCP/IP protocol as follows:

(1) First click **Properties**, then **Install** in the status window of the **LAN Connection**.

(2) Select the **Protocol** entry.

(3) Click **Add**.

(4) Select **Internet Protocol (TCP/IP)** and click on **OK**.

(5) Follow the on-screen instructions and restart your PC when you have finished.

Allocating PC IP address

Allocate an IP address to your PC as follows:

(1) Select **Internet Protocol (TCP/IP)** and click **Properties**.

(2) Choose **Use following IP address** and enter a suitable IP address, the matching netmask, your default gateway and your preferred DNS server.

If you run a DHCP server in your network, you can apply the default Windows setting **Obtain IP address automatically** and **Obtain DNS server address automatically**.

Your PC should now meet all the prerequisites for configuring your device.

2.4 IP configuration

In the ex works state, your device is configured in DHCP Client mode and therefore dynamically receives an IP address if you run a DHCP server in your network. If this is not the case, connect your device directly to the configuration PC and use the fallback IP address *192.168.0.252*.

Configuration with configuration services

Wireless LAN Controller: With the be.IP integrated in the ALL IP system and assistant guided WLAN controller, that access point can be put into operation. Please refer to your gateway's data sheet to find out the number of Access Points that you can manage with your gateway's wireless LAN controller and details of the licenses required.

When you select the **Wizard** you will receive instructions and explanations on the separate pages of the Wizard.

Cloud NetManager*: With the Cloud NetManagerhas you can manage the access points. A valid license for each access point is needed.

Note

* Cloud NetMAnager is currently in preparation!

Note

If you have previously implemented configurations on your device using the **Wireless LAN Controller**, you must set your device to delivery status before using the Cloud NetManager. The current boot-up configuration will be deleted. Do not forget to export it, if necessary, and to save it on your PC if you want to use it later.

If you are using the Cloud NetManager, you do not have access to the menus for WLAN configuartion. If you want to use the Cloud NetManager, you must disable the **Wireless LAN Controller** in advance (if it is available). Otherwise, this will take precedence.

The simultaneous operation of the Cloud Net Manager and Wireless LAN Controller is currently not intended.

In the **System Administration**-> **Global Settings** ->**System** menu, **Communication with the NetManager** is *activated*. The address of the Cloud NetManager is preconfigured in the **NetManager IP address field.** If you want to run your own management system, you need to enter the address of your server here.

Step-by-step instructions for the most important configuration tasks can be found in the separate **Application Workshop** guide for each application, which can be downloaded from our web site.

GUI Call up

Start the configuration interface as follows:

(a) Enter the IP address of your device in the address line of your Web browser.

With DHCP server:

- the IP address that the DHCP server assigned to your device

Without DHCP server:

- With direct connection to the configuration PC: the fallback IP address *192.168.0.252*

(b) Enter *admin* in the **User** field and *admin* in the **Password** field.

(c) Click **LOGIN** in order to get to the configuration interface.

2.5 Modify system password

All bintec elmeg devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. Make sure you change the passwords to prevent unauthorised access to your device!

Proceed as follows:

(a) Go to the **System Management**->**Global Settings**->**Passwords** menu.

(b) Enter a new password for **System Admin Password**.

(c) Enter the new password again under **Confirm Admin Password**.

(d) Click **OK**.

(e) Store the configuration using the **Save configuration** button above the menu navigation.

Note the following rules on password use:

- The password must not be easy to guess. Names, car registration numbers, dates of birth, etc. should not be chosen as passwords.

- The password should contain at least one character that is not a letter (special character or number).
- The password should be at least 8 characters long.
- Change your password regularly, e.g. every 90 days.

2.6 Software Update

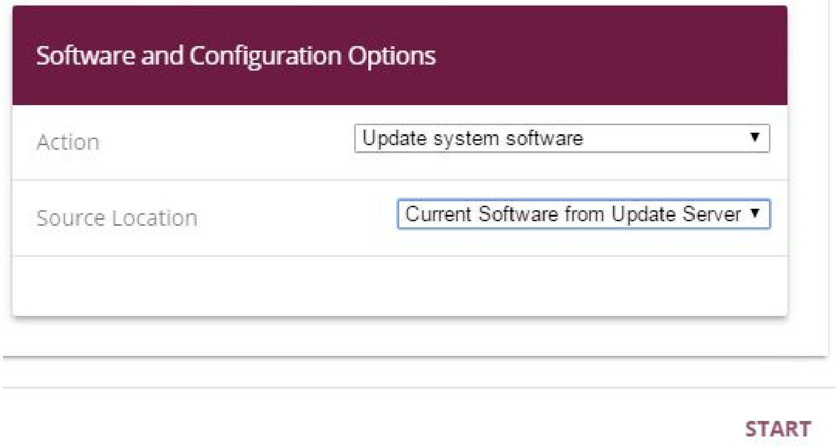
The range of functions of bintec elmeg devices is continuously being extended. These extensions are made available to you by bintec elmeg GmbH free of charge. Checking for new software versions and the installation of updates can be carried out easily with the **GUI**. An existing internet connection is needed for an automatic update.

Proceed as follows:

(1) Go to the **Maintenance**->**Software &Configuration** menu.

(2) Under **Action** select *Update System Software* and, under **Source Location** *Latest Software from Update Server.*

(3) Confirm with **Start**.



Software and Configuration Options

Action: Update system software

Source Location: Current Software from Update Server

The device will now connect to the bintec elmeg GmbH download server and check whether an updated version of the system software is available. If so, your device will be updated automatically. When installation of the new software is complete, you will be invited to restart the device.

⚠ **Caution**

After confirming with **Go**, the update cannot be aborted. If an error occurs during the update, do not re-start the device and contact support.

Chapter 3 System Management

The **System Management** menu contains general system information and settings.

You see a system status overview. Global system parameters such as the system name, date/time and passwords are managed and the authentication methods are configured.

3.1 Status

The status page displays the most important system information.

You see an overview of the following data:

- System status
- Your device's activities: Resource utilisation
- Status and basic configuration of the LAN interfaces (depending on the device)

The menu **System Management**->**Status** consists of the following fields:

Fields in the System Information menu

Field	Value
Uptime	Displays the time past since the device was rebooted.
System Date	Displays the current system date and system time.
Firmware Version	Displays the currently loaded version of the system software.
Serial Number	Displays the device serial number.
Last configuration stored	Displays day, date and time of the last saved configuration (boot configuration in flash).

Fields in the Resource Information menu

Field	Value
Memory Usage	Displays the usage of the working memory in MByte in relation to the available total working memory in MByte. The usage is also displayed in brackets as a percentage.

Fields in the Physical Interfaces menu

Field	Value
Interface - **Connection Information** - **Link**	The physical interfaces are listed here and their most important settings are shown. The system also displays whether the inter-

Field	Value
	face is connected or active. Interface specifics for Ethernet interfaces: • IP address • Netmask • Not configured

Fields in the WLAN Interface menu

Field	Value
Regulatory Domain	Display the geographical area where the device is licensed ex works. Possible value: • `ETSI`: The device is licensed for Europe.

3.2 Global Settings

The basic system parameters are managed in the **Global Settings** menu.

3.2.1 System

Your device's basic system data is entered in the **System Management**->**Global Settings**->**System** menu.

The **System Management**->**Global Settings**->**System** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Value
System Name	Enter the system name of your device. This is also used as the DHCP host name. A character string with a maximum of 255 characters is possible. The device type is entered as the default value.

Field	Value
Location	Enter the location of your device.
Contact	Enter the relevant contact person. Here you can enter the e-mail address of the system administrator, for example. A character string with a maximum of 255 characters is possible.
LED mode	Select the LEDs' lighting behaviour. Possible values: • *off* • *normal* • *minimal*
Show Manufacturer Names	Here you can determine if the manufacturer part of a MAC address is to be "translated". The manufacturer part takes up to eight characters at the beginning of the MAC address. Instead of, e.g., *00:a0:f9:37:12:c9*, *BintecCo_37:12:c9* is displayed if this option is enabled.

Fields in the menu Remote Configuration

Field	Value
NetManager communication	Select whether communication the access point is to be allowed via NetManager. The function is activated by selecting *Enabled*. The function is enabled by default.
NetManager address	Enter the NetManager IP address.
Allow configuration via WLAN Controller	Select whether configuring the access point is to be allowed via WLAN Controller. The function is activated by selecting *Enabled*. The function is enabled by default.
Obtain WLAN Controller IP Address	Only if **Allow configuration via WLAN Controller** *Enabled* Possible values:

Field	Value
	• *DHCP* (default value, function enabled): The WLAN Controller IP address assigned via a DHCP server with active CAPWAP option 138 is requested. The access point will be configured by this WLAN Controller. • *Static* (function disabled): The IP address of the WLAN Controller that is to be used for configuring the access point is entered manually.
Manual WLAN Controller IP Address	Only if **Obtain WLAN Controller IP Address** = *Static* Enter the WLAN Controller IP address.

3.2.2 Passwords

Setting the passwords is another basic system setting.

Note

All devices are delivered with the same username and password. As long as the password remains unchanged, they are not protected against unauthorised use.

Make sure you change the passwords to prevent unauthorised access to the device

The **System Management**->**Global Settings**->**Passwords** menu consists of the following fields:

Fields in the System Password menu.

Field	Value
System Admin Password	Enter the password for the user name admin. The preset value is admin. This password is saved as salted SHA-512 hash. It is used for system access by GUI.
Confirm Admin Password	Confirm the password by entering it again.

Fields in the Global Password Options menu

Field	Value
Show passwords and	Define whether the passwords are to be displayed in clear text

Field	Value
keys in clear text (if possible)	(plain text). Encryted passwords cannot be displayed in plain text. The function is enabled with *Show* The function is disabled with *Hide* The function is disabled by default. If you activate the function, all passwords and keys in all menus are displayed and can be edited in plain text if possible.

3.2.3 Date and Time

You need the system time for tasks such as correct timestamps for system messages.

You have the following options for determining the system time (local time):

Manual

The time can be set manually on the device.

If the correct location of the device (country/city) is set for the **Time Zone**, switching from summer time to winter time (and back) is automatic. This is independent of the exchange time or the ntp server time. Summer time starts on the last Sunday in March by switching from 2 a.m. to 3 a.m. The calendar-related or schedule-related switches that are scheduled for the missing hour are then carried out. Winter time starts on the last Sunday in October by switching from 3 a.m. to 2 a.m. The calendar-related or schedule-related switches that are scheduled for the additional hour are then carried out.

If a value other than Universal Time Coordinated (UTC), option *UTC+-x*, has been chosen for the **Time Zone**, the switch from summer to winter time must be carried out manually when required.

Time server

You can obtain the system time automatically, e.g. using various time servers. To ensure that the device uses the desired current time, you should configure one or more time servers. Switching from summer time to winter time (and back) must be carried out manually if the time is derived using this method by changing the value in the **Time Zone** field with an option UTC+ or UTC-.

Note

If a method for automatically deriving the time is defined on the device, the values obtained in this way automatically have higher priority. A manually entered system time is therefore overwritten.

The menu **System Management**->**Global Settings**->**Date and Time** consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Time Zone	Select the time zone in which your device is installed. You can select Universal Time or a predefined location, e. g. `Europe/Berlin`.
Current Local Time	The current date and current system time are shown here. The entry cannot be changed.

Fields in the menu Manual Time Settings

Field	Description
Set Date	Clicking into the field for adding a date brings up a standard calender. Clicking the desired date will enter it into the configuration interface.
Set Time	Enter a new time. Format: • **Hour**: hh • **Minute**: mm

Fields in the menu Automatic Time Settings (Time Protocol)

Field	Description
Update system time from time server	Determine whether the system time is to be updated via time server. The function is activated by selecting `Enabled`. The function is disabled by default.

Field	Description
First Timeserver	Only if **Update system time from time server** = `Enabled` Enter the primary time server, by using either a domain name or an IP address.
Second Timeserver	Only if **Update system time from time server** = `Enabled` Enter the secondary time server, by using either a domain name or an IP address.

3.3 Remote Authentication

This menu contains the settings for user authentication.

3.3.1 RADIUS

RADIUS (Remote Authentication Dial In User Service) is a service that enables authentication and configuration information to be exchanged between your device and a RADIUS server. The RADIUS server administrates a database with information about user authentication and configuration and for statistical recording of connection data.

RADIUS can be used for:

- Authentication
- Accounting
- Exchange of configuration data

For an incoming connection, your device sends a request with user name and password to the RADIUS server, which then searches its database. If the user is found and can be authenticated, the RADIUS server sends corresponding confirmation to your device. This confirmation also contains parameters (called RADIUS attributes), which your device uses as WAN connection parameters.

If the RADIUS server is used for accounting, your device sends an accounting message at the start of the connection and a message at the end of the connection. These start and end messages also contain statistical information about the connection (IP address, user name, throughput, costs).

RADIUS packets

The following types of packets are sent between the RADIUS server and your device (client):

Packet types

Field	Value
ACCESS_REQUEST	Client -> Server If an access request is received by your device, a request is sent to the RADIUS server if no corresponding connection partner has been found on your device.
ACCESS_ACCEPT	Server -> Client If the RADIUS server has authenticated the information contained in the ACCESS_REQUEST, it sends an ACCESS_ACCEPT to your device together with the parameters used for setting up the connection.
ACCESS_REJECT	Server -> Client If the information contained in the ACCESS_REQUEST does not correspond to the information in the user database of the RADIUS server, it sends an ACCESS_REJECT to reject the connection.
ACCOUNTING_START	Client -> Server If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the start of each connection.
ACCOUNTING_STOP	Client -> Server If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the end of each connection.

A list of all entered RADIUS servers is displayed in the **System Management**->**Remote Authentication**->**RADIUS** menu.

3.3.1.1 Edit or New

Choose the ✎ icon to edit existing entries. Choose the **New** button to add RADIUS servers. You can assign up to eight RADIUS server, one for each SSID.

The **System Management**->**Remote Authentication**->**RADIUS**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the description of the RADIUS server.
Server IP Address	Enter the IP address of the RADIUS server.
RADIUS Secret	Enter the shared password used for communication between the RADIUS server and your device. When using a Microsoft RADIUS server, the password may consist of letters, numbers, and special characters. When using an alternative RADIUS server (eg FREERADIUS), the password must not contain any special characters.

The menu **Advanced Settings** consists of the following fields:

Fields in the Server Options menu

Field	Description
Auth Port	Enter the port to be used for authentification. The default value (according to RFC 2138) is *1812*.
Acct Port	Enter the port to be used for accounting. The default value (according to RFC 2138) is *1813*.
Accounting interval	Enter the time interval (in seconds) the client is to be send update information to the RADIUS server. The default value is *180*. *0* switches the function off.

Chapter 4 LAN

In this menu, you configure the addresses in your LAN and can structure your local network using VLANs.

4.1 VLAN/Bridge Groups

4.1.1 Port Configuration

In this menu, you can define and view the rules for receiving VLAN at the ports.

4.1.1.1 Edit

Choose the ✎ icon to edit existing entries.

The **LAN**->**VLAN/Bridge Groups**->**Port Configuration**->✎ menu consists of the following fields:

Fields in the Configure Port menu

Feld	Beschreibung
VLAN ID	Enter the whole number that identifies the VLAN. Possible values: *1* to *4092* You can use the **Add** button to add more VLANs.
Description	First under **VLAN ID** = *None* enter a name for the Ethernet in the field **Description**. In all other lines, enter a unique name for the VLAN. A character string of up to 32 characters is possible.
Bridge Group	Select the bridge group that is to belong to this VLAN.

4.2 IP Configuration

In this menu, you can edit the IP configuration of the LAN and Ethernet interfaces of your device.

4.2.1 Interfaces

The existing IP interfaces are listed in the **LAN**->**IP Configuration**->**Interfaces** menu. You can edit the IP configuration of the interfaces or create virtual interfaces for special applications. Here is a list of all of the interfaces (logical Ethernet interfaces and others created in the subsystems).

Use the ✎ to edit the settings of an existing interface (bridge groups, Ethernet interfaces in routing mode).

You can use the **New** button to create virtual interfaces. However, this is only needed in special applications.

Depending on the option selected, different fields and options are available. All the configuration options are listed below.

Change the status of the interface by clicking the ˄ or the ˅ button in the **Action** column.

Press the 🔍 button to display the details of an existing interface.

Note

For IPv4 note that:

If your device has obtained an IP address dynamically from a DHCP server operated in your network for the basic configuration, the default IP address is deleted automatically and your device will no longer function over this address.

Example of subnets

If your device is connected to a LAN that consists of two subnets, you should enter a second **IP Address / Netmask**.

The first subnet has two hosts with the IP addresses 192.168.42.1 and 192.168.42.2, for example, and the second subnet has two hosts with the IP addresses 192.168.46.1 and 192.168.46.2. To be able to exchange data packets with the first subnet, your device uses the IP address 192.168.42.3, for example, and 192.168.46.3 for the second subnet. The netmasks for both subnets must also be indicated.

4.2.1.1 Edit or New

Choose the ✎ icon to edit existing entries. Choose the **New** button to create virtual interfaces.

The **LAN**->**IP Configuration**->**Interfaces**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description of the interface.
Based on Ethernet Interface	This field is only displayed if you are editing a virtual routing interface. Select the Ethernet interface for which the virtual interface is to be configured.
Interface Mode	Only for physical interfaces in routing mode and for virtual interfaces. The configuration mode of the *Tagged (VLAN)* interface is displayed. You use this option to assign the interface to a VLAN. This is done using the VLAN ID, which is displayed in this mode and can be configured. The definition of a **MAC Address** is optional in this mode.
VLAN ID	Only for **Interface Mode** = *Tagged (VLAN)* This option only applies for routing interfaces. Assign the interface to a VLAN by entering the VLAN ID of the relevant VLAN. Possible values are *1* (default value) to *4092*.
MAC Address	Enter the MAC address associated with the interface. For virtual interfaces, you can use the MAC address of the physical interface under which the virtual interface was created by activating **Use built-in**, but VLAN IDs must be different. You can also allocate a virtual MAC address. If **Use built-in** is active, the predefined MAC address of the al-

Field	Description
	located physical interface is used. **Use built-in** is activated by default.
Address Mode	Select how an IP address is assigned to the interface. Possible values: • *Static* (default value): You can assigen a static IP address to the interface in **IP Address / Netmask**. • *DHCP*: An IP address is assigned to the interface dynamically via DHCP.
IP Address / Netmask	Only for **Address Mode** = *Static* With **Add**, add a new address entry and enter the **IP Address** and the corresponding **Netmask** of the virtual interface. You can add several address entries. If you want to configure your device via this interface, you have to assign an IP address to the interface.

Chapter 5 Wireless LAN

In the case of wireless LAN or **Wireless LAN** (WLAN = Wireless Local Area Network), this relates to the creation of a network using wireless technology.

Network functions

Like a wired network, a WLAN offers all the main network functions. Access to servers, files, printers, and the e-mail system is just as reliable as company-wide Internet access. Because the devices do not require any cables, the great advantage of WLAN is that there are no building-related restrictions (i.e. the device location does not depend on the position and number of connections).

Currently applicable standard: IEEE 802.11ac. Information on the modes contained in the standard and the correspondingly supported transmission speeds are, e.g., avilable at *Wikipedia*. Pay attention to the security and conformity information provided with your product!

5.1 WLAN

In the **Wireless LAN**->**WLAN** menu, you can configure all WLAN modules of your device.

Your devices **W2022ac** and **W2022ac-ext** have two WLAN modules **WLAN** 1 (Operation Band 2.4 GHz) and **WLAN** 2 (Operation Band 5 GHz).

5.1.1 Radio Settings

In the **Wireless LAN**->**WLAN**->**Radio Settings** menu, an overview of the configuration options for the WLAN module is displayed.

5.1.1.1 Radio Settings-> ✎

In this menu, you change the settings for the wireless module.

The **Wireless LAN**->**WLAN**->**Radio Settings**-> ✎ menu consists of the following fields:

Fields in the menu Wireless Settings

Field	Description
Operation Mode	Define the mode in which the wireless module of your device is

Field	Description
	to operate. Possible values: • *Off* (default value): The wireless module is not active. • *Access-Point*: Your device serves as an Access Point in your network.
Operation Band	**WLAN1** = *2.4 GHz* This value is only displayed in the overview and can not be changed. For **WLAN2** = *5 GHz* • Operation Band *5 GHz Indoor*, • Operation Band *5 GHz Outdoor*, • Operation Band *5 GHz Indoor-Outdoor* (default value)
Channel	In the case of manual channel selection, please make sure first that the clients actually support these channels. Possible values: • For **Operation Band** = *2.4 GHz* Possible values are *Auto* (default value) and *1* to *13* . • For **Operation Band** = *5 GHz Indoor* Possible values: *Auto* (default value) and *36*, *40*, *44*, *48* • For **Operation Band** = *5 GHz Indoor-Outdoor* or *5 GHz Outdoor* Possible value: *Auto*
Transmit Power	Select the maximum value for the radiated antenna power. The actually radiated antenna power may be lower than the maximum value set, depending on the data rate transmitted. Possible values: For **Operation Band** = *2.4 GHz* • *5 dBm* to

Field	Description
	• *20 dBm* (default value) For **Operation Band** = *5 GHz Indoor / 5 GHz Outdoor / 5 GHz Indoor-Outdoor* • *5 dBm* to • *23 dBm* (default value)

Fields in the menu Performance Settings

Field	Description
Wireless Mode	Select the wireless technology that the access point is to use. There are also settings combining two or three WLAN standards. For **Operation Band** = *2.4 GHz* Possible values: • *802.11b/g/n*: Devices which operate according to *802.11b*, *802.11g* or *802.11n* have access. • *802.11b/g*: Devices which operate according to *802.11b* or *802.11g* have access. • *802.11g/n* (default value): Devices which operate according to *802.11g* or *802.11n* have access. • *802.11n*: Your device operates only according to 802.11n. • *802.11b*: Your device operates only in accordance with 802.11b and forces all clients to adapt to it. • *802.11g*: Your device operates only according to 802.11g. 802.11g. 802.11b clients have no access For **Operation Band** = *5 GHz* Possible values: • *802.11a/n/ac* (default value): Devices which operate according to *802.11a*, *802.11n* or *802.11ac* have access. • *802.11n/ac*: Devices which operate according to *802.11n* or *802.11ac* have access. • *802.11a/n*: Devices which operate according to *802.11a* or *802.11n* have access.

Field	Description
	• *802.11ac*: Your device operates according to either 802.11ac. • *802.11n*: Your device operates only according to 802.11n. • *802.11a*: The device operates only in accordance with 802.11a.
Number of Spatial Streams	For **Operation Band** = *5 GHz Indoor-Outdoor* and not **Wireless Mode** *802.11a* Select how many traffic flows are to be used in parallel. Possible values: • *2*: Two traffic flows are used. • *1*: One traffic flow is used.
Bandwidth	For **Operation Band** = *5 GHz* and not **Wireless Mode** *802.11a* Select how many channels are to be used. Possible values: • *20 MHz* (default value): One channel with 20 MHz bandwidth is used. • *40 MHz*: Two channels each with 20 MHz bandwidth are used. In the case one channel acts as a main channels and the other as an expansion channel. • *80 MHz*: Vour channels each with 20 MHz bandwidth are used. Thus, a bandwidth of 80 MHz is available.
Cyclic Background Scanning	You can enable the **Cyclic Background Scanning** function so that a search is run at regular intervals for neighbouring or rogue access points in the network. This search is run without negatively impacting the function as an access point. Enable or disable the function **Cyclic Background Scanning**. The function is enabled with *Enabled*. The function is not activated by default.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Channel Plan	Select the desired channel plan. The so-called channel plan allows the automatic selection of channels based on specific choices. This ensures that channels do not overlap, i.e. a gap of four channels is maintained between the channels used. This is useful if multiple access points with overlapping radio cells are used. Possible values: • *All*: All channels can be chosen during channel selection. • *World Mode* (for **Operation Band** = *2.4 GHz*, default value): Automatic channel selection uses only the non-overlapping channels *1*, *6*, *11*. • *ETSI Mode* (for **Operation Band** = *2.4 GHz*): Automatic channel selection uses only the non-overlapping channels *1*, *5*, *9*, *13*. • *No weather radar channels* (for **Operation Band** = *5 GHz*, default value): The weather radar channels are excluded from channel selection. Possible values: *36*, *40*, *44*, *48*, *52*, *56*, *60*, *64*, *100*, *104*, *108*, *112*, *116*, *132*, *136*, *140*. • *Indoors No DFS/TPC*: These channels can be used inside buildings. DFS (Dynamic Frequency Selection) and TPC (Transmitter Power Control) are not enabled. Possible values: *36*, *40*, *44*, *48*. • *User defined*: Select the desired channels.
Selected Channels	Only for **Channel Plan** = *User defined* The currently selected channels are displayed here. You can activate or deactivate individual channels.
Beacon Period	For **Operation Band** = *2.4 GHz*

Field	Description
	Enter the time in milliseconds between the sending of two beacons. Possible values are `40` to `3500`. The default value is `100`.
Short Guard Interval	Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800 ns to 400 ns. The function is activated by default.

5.1.2 Wireless Networks (VSS)

If you are operating your device in Access Point Mode (**Wireless LAN**->**WLAN**->**Radio Settings**-> ✎ ->**Operation Mode** = `Access Point`), in the menu **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)**->✎ **/ New** you can edit the wireless networks required or set new ones up.

Setting network names

In contrast to a LAN set up over Ethernet, a wireless LAN does not have any cables for setting up a permanent connection between the server and clients. Access violations or faults may therefore occur with directly adjacent radio networks. To prevent this, every radio network has a parameter that uniquely identifies the network and is comparable with a domain name. Only clients with a network configuration that matches that of your device can communicate in this WLAN. The corresponding parameter is called the network name. In the network environment, it is sometimes also referred to as the SSID.

Protection of wireless networks

As data can be transmitted over the air in the WLAN, this data can in theory be intercepted and read by any attacker with the appropriate resources. Particular attention must therefore be paid to protecting the wireless connection.

The security modes WPA-PSK and WPA Enterprise are available. WPA Enterprise offers the highest level of security, but this security mode is geared at enterprises, because it requires a central authentication server. Private users should choose choose WPA-PSK with only WPA2 and AES for optimal security, as well as assign a secure at least 8-digit WLAN password.

WPA

WPA (Wi-Fi Protected Access) offers additional privacy by means of dynamic keys, and offers PSK (preshared keys) or Extensible Authentication Protocol (EAP) via 802.1x (e.g. RADIUS) for user authentication.

Authentication using EAP is usually used in large wireless LAN installations, as an authentication instance in the form of a server (e.g. a RADIUS server) is used in these cases. PSK (preshared keys) are usually used in smaller networks, such as those seen in SoHo (Small office, Home office). Therefore, all the wireless LAN subscribers must know the PSK, because it is used to generate the session key.

WPA 2

The extansion and the successor of **WPA** is **WPA 2**. In **WPA 2**, the 802.11i standard is implemented for the first time in full.

Access control

You can control which clients can access your wireless LAN via your device by creating an Access Control List (**Access Control** oder **MAC-Filter**). In the Access Control List, you enter the MAC addresses of the clients that may access your wireless LAN. All other clients have no access.

Security measures

To protect the data transferred over the WLAN, the following configuration steps should be carried out in the **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)**->**New** menu, where necessary:

- Change the access passwords for your device.
- Set **Visible** = *Enabled*. This will exclude all WLAN clients that attempt to establish a connection with the general value for **Network Name (SSID)** *Any* and do not know the SSID settings.
- Use the available encryption methods. To do this, select **Security Mode** = *WPA-PSK* or *WPA Enterprise* and enter the relevant key in the access point under **Preshared Key** and in the WLAN clients.
- For transmission of information with very high security relevance, configure **Security Mode** = *WPA Enterprise* with **WPA Mode** = *WPA 2*. This method contains encryption and RADIUS authentication of the client.
- Restrict WLAN access to permitted clients. Enter the MAC addresses of the wireless network cards for these clients in the **Allowed Addresses** list in the **MAC-Filter** menu (see *Fields in the menu MAC-Filter* on page 40).

A list of all WLAN networks is displayed in the **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)** menu.

5.1.2.1 Edit or New

Choose the ✎ icon to edit existing entries. Choose the **New** button to configure additional wireless networks.

The **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)**-> ✎ **/ New** menu consists of the following fields:

Fields in the menu Service Set Parameters

Field	Description
Description	Enter a description for the access point.
Network Name (SSID)	Enter the name of the wireless network (SSID). Enter an ASCII string with a maximum of 32 characters. Select whether the **Network Name (SSID)** is to be transmitted. The network name is displayed by selecting *Visible*. It is visible by default.
Intra-cell Repeating	Select whether communication between the WLAN clients is to be permitted within a radio cell. The function is activated by selecting *Enabled*. The function is enabled by default.
WMM	Select whether voice and video prioritization via WMM (Wireless Multimedia) is to be activated for the wireless network so that optimum transmission quality is maintained for time-critical applications. Data prioritization is supported in accordance with DSCP (Differentiated Services Code Point) or IEEE802.1d. The function is enabled by default. If **Wireless Mode** *802.11a* , *802.11b* or *802.11g* is selected, the function can be disabled. For all other settings for the **Wireless Mode** parameter (*802.11n* or *802.11ac*, for example),

Field	Description
	WMM is always active and the deactivation button is greyed out.

Fields in the menu Bridge Group settings

Field	Description
Bridge Group	Select an existing bridge group (`br0`, `br1` etc.), a new bridge group (*`New`*) or none bridge group (*`None`*).

Fields in the menu Security Settings

Field	Description
Security Mode	Select the **Security Mode** (encryption and authentication) for the wireless network. Possible values: • *`OWE-Transition`*: ☞ **Note** Please note: if you want to use *`OWE-Transition`*, you must first configure a **Wireless Network (VSS)** with a self-chosen SSID and the **Security Mode** *`inactive`* as a basis. Then, you can configure the OWE transition network selecting this base network under **Base Network (SSID)**. This connects these networks. The security mode of the open OWE transition network can not be changed. After deleting or changing the security mode of the base network or selecting another base network, you can change the security mode of the OWE transition network again. If the open basic network is deleted, an OWE network remains instead of the OWE transition network. If the OWE transition network is deleted, an open basic network remains. The *`OWE-Transition`* setting does not require the input of a **Preshared Key** and is suitable for open guest networks. Data transmission between access point and client is encrypted for clients supporting **WPA3**. For clients not supporting **WPA3**, data transmission is unencypted. • *`OWE`*

Field	Description
	Note OWE only works with clients supporting WPA3. The *OWE* setting does not require the input of a **Preshared Key** and is suitable for open guest networks. Nevertheless, data transmission between the access point and the clients is encrypted. • *Inactive* : Neither encryption nor authentication • *WPA-PSK* (default value): WPA Preshared Key • *WPA Enterprise*: 802.11i/TKIP
WPA Mode	For **Security Mode** = *WPA-PSK* and *WPA Enterprise* Possible values: • *WPA*: WLAN clients that support **WPA** can connect. • *WPA2*: WLAN clients that support **WPA2** can connect. • *WPA3*: Only WLAN clients that support **WPA3** can connect. • *WPA and WPA2* : WLAN clients that support **WPA1** or **WPA2** can connect. • *WPA2 and WPA3* (default value): WLAN clients that support **WPA2** or **WPA3** can connect.
Base Network (SSID)	For **Security Mode** = *OWE-Transition* Specify which network is to be used as a basis for an OWE transition network. Select the SSID of a network configured with **Security Mode** = *inactive* (see note under parameter **Security Mode** in section *OWE-Transition*).
WPA Cipher	For **Security Mode** = *WPA-PSK* or *WPA Enterprise* and for **WPA Mode** = *WPA* or *WPA and WPA2* Select the type of encryption you want to apply. Possible values:

Field	Description
	• *AES* : AES is used. • *TKIP*: TKIP is used. • *AES and TKIP* (default value): AES or TKIP is used.
WPA2 Cipher	For **Security Mode** = *WPA-PSK* or *WPA Enterprise* and for **WPA Mode** = *WPA2* or *WPA and WPA2* Select the type of encryption you want to apply. Possible values: • *AES* : AES is used. • *AES and TKIP* (default value): AES or TKIP is used.
Preshared Key	Only for **Security Mode** = *WPA-PSK* Enter the WPA password. Enter an ASCII string with 8 - 63 characters. ☞ **Note** Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!
RADIUS Server	Only for **Security Mode** = *WPA Enterprise* You can control access to a wireless network via a RADIUS server. You can select from the RADIUS servers configured under **System Management**->**Remote Authentication**->**RADIUS**->**New** .

Fields in the menu Client load balancing

Field	Description
Max. number of clients - hard limit	Enter the maximum number of clients that can be connected to this wireless network (SSID) The maximum number of clients that can register with a wireless module depends on the specifications of the respective WLAN module. This maximum is distrubuted across all wireless

Field	Description
	networks configured for this radio module. No more new wireless networks can be created and a warning message will appear if the maximum number of clients is reached. Possible values are whole numbers between *1* and *255*. The default value is *32*.
Max. number of clients - soft limit	To avoid a radio module being fully utilised, you can set a "soft" restriction on the number of connected clients. If this number is reached, new connection queries are initially rejected. If the client cannot find another wireless network and, therefore, repeats its query, the connection is accepted. Queries are only definitively rejected when the **Max. number of clients - hard limit** is reached. The value of the **Max. number of clients - soft limit** must be the same as or less than that of the **Max. number of clients - hard limit**. The default value is *28*. You can disable this function if you set **Max. number of clients - soft limit** and **Max. number of clients - hard limit** to identical values.
Client Band select	Select whether the 5 GHz band is preferred. Possible values: • *Disabled - optimized for fast roaming*: the 5 GHz band is not preferred, fast roaming is used. • *5 GHz band preferred*: the 5 GHz band is preferred to be used if available. ☞ **Note** For the *5 GHz band preferred* setting, configure the same SSID in both client bands.

Fields in the menu MAC-Filter

Field	Description
Access Control	Select whether only certain clients are to be permitted for this wireless network. The function is activated by selecting *Enabled*. The function is disabled by default.
Allowed Addresses	Only for **Access Control** *Enabled* Use **Add** to make entries and enter the MAC addresses (**MAC Address**) of the clients to be permitted.

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
DTIM Period	Enter the interval for the Delivery Traffic Indication Message (DTIM). The DTIM field is a data field in transmitted beacons that informs clients about the window to the next broadcast or multicast transmission. If clients operate in power save mode, they come alive at the right time and receive the data. Possible values are *1* to *100*. The default value is *2*.
Group Rekeying	The Group Key encrypts data which is to be sent to all connected clients (broadcast).
Rekeying Intervall	Only for **Group Rekeying** = *Enabled* Enter the interval (in seconds) after which the group key is renewed. Possible values are *30* to *86400* The default value ist *86400*.

Fields in the menu Data-rate trimming

Field	Description
2,4 GHz band rate pro-	Data Rate Trimming allows you to optimize the performance of

Field	Description
file	your wireless LAN. You can block low transfer rates and enforce the use of higher rates. Clients slowing down other clients through the use of low transfer rates are disconnected from the access point. Select the rate profile to be applied: • *All (Min. 1 MBit/s)* - All clients supporting a transfer rate of 1 MBit/s are allowed to connect to the access point. • *Min. 6 MBit/s (no 802.11b devices)*- see above, for clients with a minimum supported rate of 6 Mbit/s; clients using the obsolete standard 802.11b are not allowed. • *Min. 12 MBit/s (keine 802.11b-Geräte)*- see above, for clients with a minimum supported rate of 12 Mbit/s • *Min. 24 MBit/s (keine 802.11b-Geräte)*- see above, for clients with a minimum supported rate of 24 Mbit/s
5 GHz band rate profile	Possible values: • *All (Min. 6 MBit/s)* - All clients supporting a transfer rate of 6 MBit/s are allowed to connect to the access point. • *From 12 MBit/s* - see above, for clients with a minimum supported rate of 12 Mbit/s • *From 24 MBit/s* - see above, for clients with a minimum supported rate of 24 Mbit/s

Fields in the menu SNR Threshold Management

Field	Description
SNR Threshold Management	Activate this option to define the minimum need signal quality required for setting up the wireless connection. The function is disabled by default.
SNR Threshold	Only for **SNR Threshold Management** = *Enabled* The SNR Threshold parameter allows you to define a limit value for signal-to-noise ratio when communicating with a client. If an access point "sees" that one of its clients falls below this signal-to-noise ratio for longer than the tolerance time specified, it disconnects from the client. This forces the client to look for a new access point, i.e. to check which access point provides the best

Field	Description
	signal and connect to it. Enter the SNR threshold in dB. If this value is longer than under the tolerance time is exceeded, the access point disconnects the connection to the affected client. The default valuet is *1* dB, this deactivates the function. Low SNR thresholds determine that the connection to the client will be disconnected only at long distances. High SNR thresholds indicate that the connection is already disconnected at a smaller distance to the client. A practicable value is an SNR of 40 dB.
Grace time	Only for **SNR Threshold Management** = *Enabled* Enter the time (in seconds) during which the data transfer rate may drop below the SNR threshold without the client having to calculate consequences. The default value is *5* seconds.

Chapter 6 Networking

6.1 Routes

Default Route

With a default route, all data is automatically forwarded to one connection if no other suitable route is available. If you do not use DHCP, enter the LAN IP address of your internet access router as the default router. If, for example, you configure both Internet access and a corporate network connection, enter a default route to the internet access router and a network route to the head office. You can enter several default routes on your device, but only one default route can be active at any one time. If you enter several default routes, you should thus note differing values for **Distance**.

6.1.1 IPv4 Route Configuration

A list of all configured routes is displayed in the **Network**->**Routes**->**IPv4 Route Configuration** menu.

6.1.1.1 Edit or New

Choose the ✎ icon to edit existing entries. Choose the **New** button to create additional routes.

The **Network**->**Routes**->**IPv4 Route Configuration**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Route Type	Select the type of route. Possible values: • *Default Route via Gateway*: Route via a specific gateway which is to be used if no other suitable route is available. • *Host Route via Gateway*: Route to an individual host via a specific gateway. • *Network Route via Gateway*: Route to a network via a

Field	Description
	specific gateway.

Fields in the menu Route Parameters

Field	Description
Destination IP Address/Netmask	Enter the IP address of the destination host or destination network. Also enter the relevant netmask in the second field.
Gateway IP Address	Enter the IP address of the gateway to which your device should forward the IP packets.
Distance	Select the distance of the route. The lower the value, the higher the priority of the route. Value range from `0` to `15`. The default value is `1`.

Chapter 7 Local Services

This menu offers services for the following application areas:

7.1 DNS

Each device in a TCP/IP network is usually located by its IP address. Because host names are often used in networks to reach different devices, it is necessary for the associated IP address to be known. This task can be performed by a DNS server, which resolves the host names into IP addresses. Alternatively, name resolution can also take place over the HOSTS file, which is available on all PCs.

7.1.1 DNS Servers

A list of all configured DNS servers is displayed in the **Local Services**->**DNS**->**DNS Servers** menu.

7.1.1.1 Add

Select the **Add** button to add the IP address of the DNS server.

7.1.2 Static Hosts

A list of all configured static hosts is displayed in the **Local Services**->**DNS**->**Static Hosts** menu.

7.1.2.1 New

Choose the **New** button to set up new static hosts.

The menu **Local Services**->**DNS**->**Static Hosts**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
DNS Hostname	Enter the host name to which the **IP Address** defined in this menu is to be assigned if a positive response is sent upon a DNS request. If a negative response is sent upon a DNS request, no address is specified.

Field	Description
	The entry can also start with the wildcard *, e.g. *.bintec-elmeg.com. If you specify a simple name (e.g. `router`), it is expanded by the Default Domain to form a complete DNS name (Fully Qualified Domain Name, FQDN). If you enter a name with the structure of a FQDN (i.e. character sequences separated by "."), the entry is interpreted as a FQDN and is not expanded. The closing "." which is mandatory for a complete FQDN is automatically appended if required. Entries with spaces are not allowed.
IP Address	Enter the IP address assigned to **DNS Hostname**.
Short Name	Enter a short name with **Add**.

Chapter 8 Maintenance

This menu provides functions for maitaining your device. It firstly provides a menu for testing availability within the network. You can manage your system configuration files. If more recent system software is available, you can use this menu to install it. If you need additional languages for the configuration interface, you can import a corresponding language pack. You can also trigger a system reboot and factory reset in this menu.

8.1 Diagnostics

In the **Maintenance**->**Diagnostics** menu, you can test the availability of individual hosts, the resolution of domain names and certain routes.

8.1.1 Ping Test

You can use the ping test to check whether a certain host in the LAN or an internet address can be reached.

Pressing the **Go** button starts the ping test. The **Output** field displays the ping test messages.

8.1.2 DNS Test

The DNS test is used to check whether the domain name of a particular host is correctly resolved. The **Output** field displays the DSN test messages. The ping test is launched by entering the domain name to be tested in **DNS Address** and clicking the **Go** button.

8.1.3 Traceroute Test

You use the traceroute test to display the route to a particular address (IP address or domain name), if this can be reached.

Pressing the **Go** button starts the Traceroute test. The **Output** field displays the traceroute test messages.

8.2 Software & Configuration

You can use this menu to manage the software version of your device, your configuration files and the language of the **GUI**.

8.2.1 Options

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You may therefore need to carry out a software update.

Every new system software includes new features, better performance and any necessary bug fixes from the previous version. You can find the current system software in the download area of our web site. The current documentation is also available here.

> ⚠ **Important**
>
> If you want to update your software, make sure you consider the corresponding release notes. These describe the changes implemented in the new system software.
>
> The result of an interrupted update (e.g. power failure during the update) could be that your gateway no longer boots. Do not turn your device off during the update.

Flash

Flash memories provide nonvolatile data storage, that is, data remains stored in the flash even when your device is switched off. They are a type of EEPROM (Electrically Erasable Programmable Read Only Memory).

RAM

The current configuration and all changes you set on your device during operation are stored in the working memory (RAM). The contents of the RAM are lost if the device is switched off. So if you modify your configuration and want to keep these changes for the next time you start your device, you must save the modified configuration in the flash memory before switching off using the **Save configuration** button over the navigation area of the **GUI**. This configuration is then saved in flash in a file named `config.boot`. When you start your device, the `config.boot` configuration file is used by default.

Actions

The files in the flash memory can be copied, moved, erased and newly created. It is also possible to transfer configuration files between your device and a host via HTTP.

The **Maintenance**->**Software &Configuration**->**Options** menu consists of the following fields:

Fields in the Currently Installed Software menu.

Field	Description
Firmware Version	Shows the current software version loaded on your device.
Bootloader Version	Shows the current boot loader version loaded on your device.
WLAN Firmware	Shows the current WLAN firmware version loaded on your device.
Software License Information	Use the **Show** button to display software license information in a separate window. You can print this information.

Fields in the Software and Configuration Options menu.

Field	Description
Action	Select the action you wish to execute. After each task, a window is displayed showing the other steps that are required. Possible values: • `No Action` (default value): • `Export configuration`: The configuration file **Current File Name in Flash** is transferred to your local host. If you click the **Go** button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name. • `Import configuration`: Under **Filename** select a configuration file you want to import. Please note: Click **Go** to first load the file under the name `boot` in the flash memory for the device. You must restart the device to enable it. • `Copy configuration`: The configuration file in the **Source File Name** field is saved as **Destination File Name**. • `Delete configuration`: The configuration in the **Select file** field is deleted. • `Update system software`: Sie können eine Aktualisierung der Systemsoftware, der Logik und des BOOTmonitors initiieren.

Field	Description
Current File Name in Flash	Only for **Action** = *Export configuration* Select the configuration file to be exported.
Filename	Only for **Action** = *Import configuration* and *Update system software* Enter the path and name of the file or select the file with **Browse...** via the explorer/finder.
Source File Name	Only for **Action** = *Copy configuration* Select the source file to be copied.
Destination File Name	Only for **Action** = *Copy configuration* Enter the name of the copy.
Select file	Only for **Action** = *Delete configuration* Select the configuration to be deleted.
Allow Software Downgrade	Only for **Action** = *Update system software* Enable or disable the option **Allow Software Downgrade** . The function is enabled with *Enabled*. The function is enabled by default.
Source Location	Only for **Action** = *Update system software* Select the source of the update. Possible values: • *Local File* (default value): The system software file is stored locally on your PC. • *External Server* : The file is stored on a remote server specified in the URL. • *Current Software from Update Server*: The file is on the official update server.
URL	Only for **Source Location** = *External Server*

Field	Description
	Enter the URL of the server from which the system software file is loaded.

In the **Advanced Settings** menu, the version of the currently installed system flash files will be displayed.

8.3 Reboot

8.3.1 System Reboot

In this menu, you can trigger an immediate reboot of your device. Once your system has restarted, you must call the **GUI** again and log in.

Pay attention to the LEDs on your device. For information on the meaning of the LEDs, see the **Technical Data** chapter of the manual.

Note

Before a reboot, make sure you confirm your configuration changes by clicking the **Save configuration** button, so that these are not lost when you reboot.

If you wish to restart your device, click the **OK** button. The device will reboot.

8.4 Factory Reset

In the menu **Maintenance**->**Factory Reset**, you can reset your device via GUI to the ex works state.

Note

Note that resetting the device to the ex-works state also deletes all additionally installed GUI language and help files. These have to be reinstalled. In order to save any installed language packs, you can try to reboot the device or delete its configuration before reseeting to the ex-works state.

Chapter 9 External Reporting

9.1 SIA

9.1.1 SIA

In the menu **External Reporting**->**SIA**->**SIA**, you can create and download a file that provides extensive support information about the status of your device like, e.g., the current configuration, available memory, uptime etc.

Chapter 10 Monitoring

This menu contains information that enable you to locate problems in your network.

10.1 Interfaces

10.1.1 Statistics

In the **Monitoring**->**Interfaces**->**Statistics** menu, current values and activities of all device interfaces are displayed.

Change the status of the interface by clicking the ⌃ or the ⌄ button in the **Action** column.

Values in the Interfaces list

Field	Description
No.	Shows the serial number of the interface.
Description	Displays the name of the interface.
Type	Displays the interface text.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Tx Errors	Shows the total number of errors sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.
Rx Errors	Shows the total number of errors received.
Status	Shows the operating status of the selected interface.
Unchanged for	Shows the length of time for which the operating status of the interface has not changed.
Action	Enables you to change the status of the interface as displayed.

Click the 🔍 button to display the statistical data for the individual interfaces in detail.

Values in the Interface Status list

Field	Description
Description	Displays the name of the interface.

Field	Description
MAC Address	Displays the MAC address.
IP Address / Netmask	Shows the IP address and the netmask.
NAT	Indicates if NAT is activated for this interface.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.

Fields in the TCP Connections list

Field	Description
Status	Displays the status of an active TCP connection.
Local Address	Displays the local IP address of the interface for an active TCP connection.
Local Port	Displays the local port of the IP address for an active TCP connection.
Remote Address	Displays the IP address to which an active TCP connection exists.
Remote Port	Displays the port to which an active TCP connection exists.

10.1.2 Network Status

The menu **Monitoring**->**Interfaces**->**Network Status** provides an overview of all IP interfaces currently configured on the device. You can find information on the status of an interface as well as on relevant parameters like its IP address, the MAC address of the interface and the currently valid MTU.

10.2 WLAN

10.2.1 VSS

In the **Monitoring**->**WLAN**->**VSS** menu, current values and activities of the configured wireless networks are displayed.

Values in the Client Node Table list

Field	Description
MAC Address	Shows the MAC address of the associated client.
IP Address	Shows the IP address of the client.
Uptime	Shows the time in hours, minutes and seconds for which the client is logged in.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
Transmit Power	Shows the strength of the received signal in dBm.
Noise dBm	Shows the received noise strength in dBm.

VSS - Details for Connected Clients

In the **Monitoring**->**WLAN**->**VSS**->**<Connected Client>** -> 🔍 menu, the current values and activities of a connected client are shown.

Values in the list <Connected Client>

Field	Description
MAC Address	Shows the MAC address of the associated client.
IP Address	Shows the IP address of the client.
Uptime	Shows the time in hours, minutes and seconds for which the client is logged in.
Tx Packets	Shows the number of sent packets for the data rate.
Rx Packets	Shows the number of received packets for the data rate.
Transmit Power	Shows the strength of the received signal in dBm.
Noise dBm	Shows the received noise strength in dBm.

10.2.2 Neighbor APs

In the **Monitoring**->**WLAN**->**Neighbor APs** menu, the adjacent AP's found during the scan are displayed. **Rogue APs**, i.e. APs which are not managed by the WLAN controller but are using an SSID managed by the WLAN controller are highlighted in red.

Note

Check the rogue APs shown carefully, as an attacker could attempt to spy on data in your network using a rogue AP.

Although each AP is found more than once, it is only displayed once with the strongest signal. You see the following parameters for each AP: **SSID**, **MAC Address**, **Channel**, **Security**.

The entries are displayed in alphabetical order by **SSID**. **Security** shows the security settings of the AP.

Index